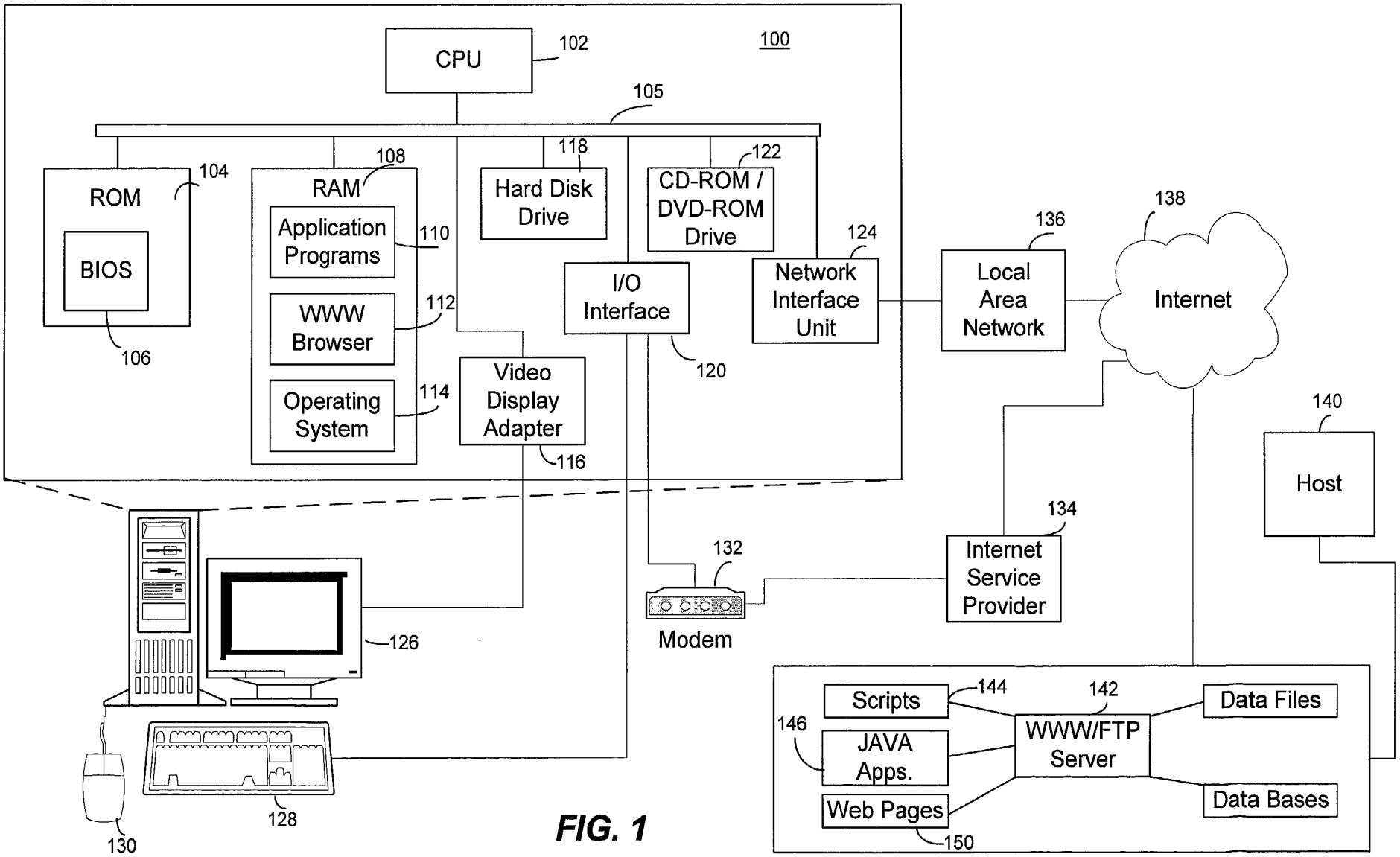
CPU
102
100
105
ROM
104
BIOS
106
RAM
108
Application Programs
110
WWW Browser
112
Operating System
114
Hard Disk Drive
118
CD-ROM / DVD-ROM Drive
122
I/O Interface
120
Network Interface Unit
124
Video Display Adapter
116
Local Area Network
136
Internet
138
Host
140
Internet Service Provider
134
Modem
132
126
128
130
Scripts
144
142
Data Files
146
JAVA Apps.
WWW/FTP Server
Data Bases
Web Pages
150

FIG. 1

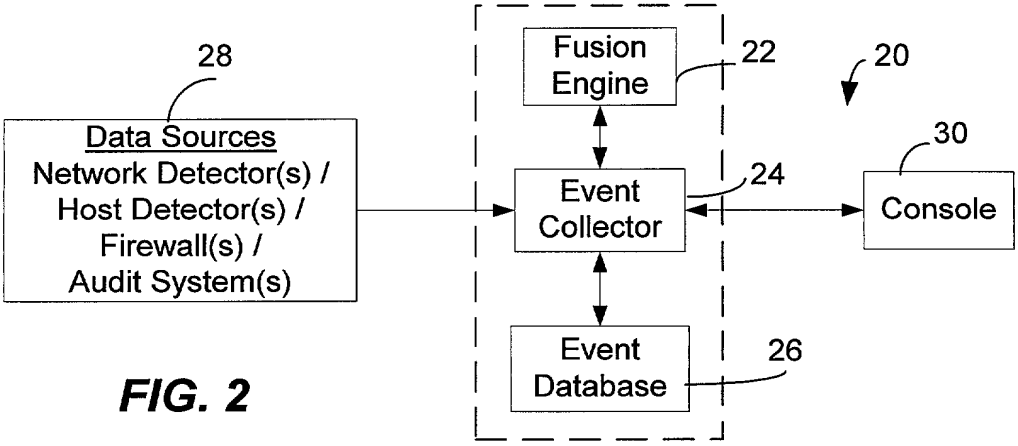

FIG. 2

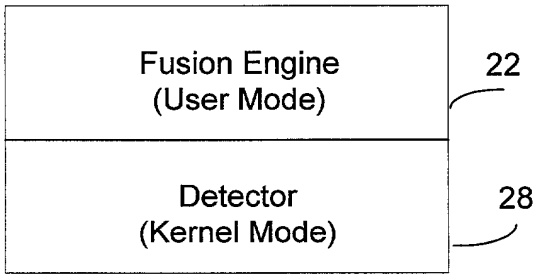

FIG. 3

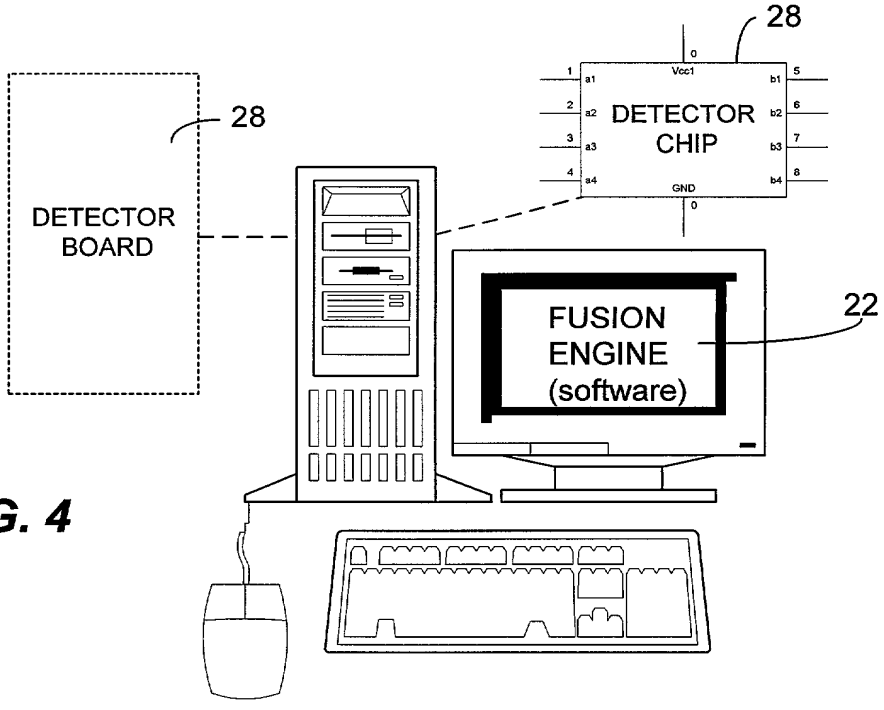

FIG. 4

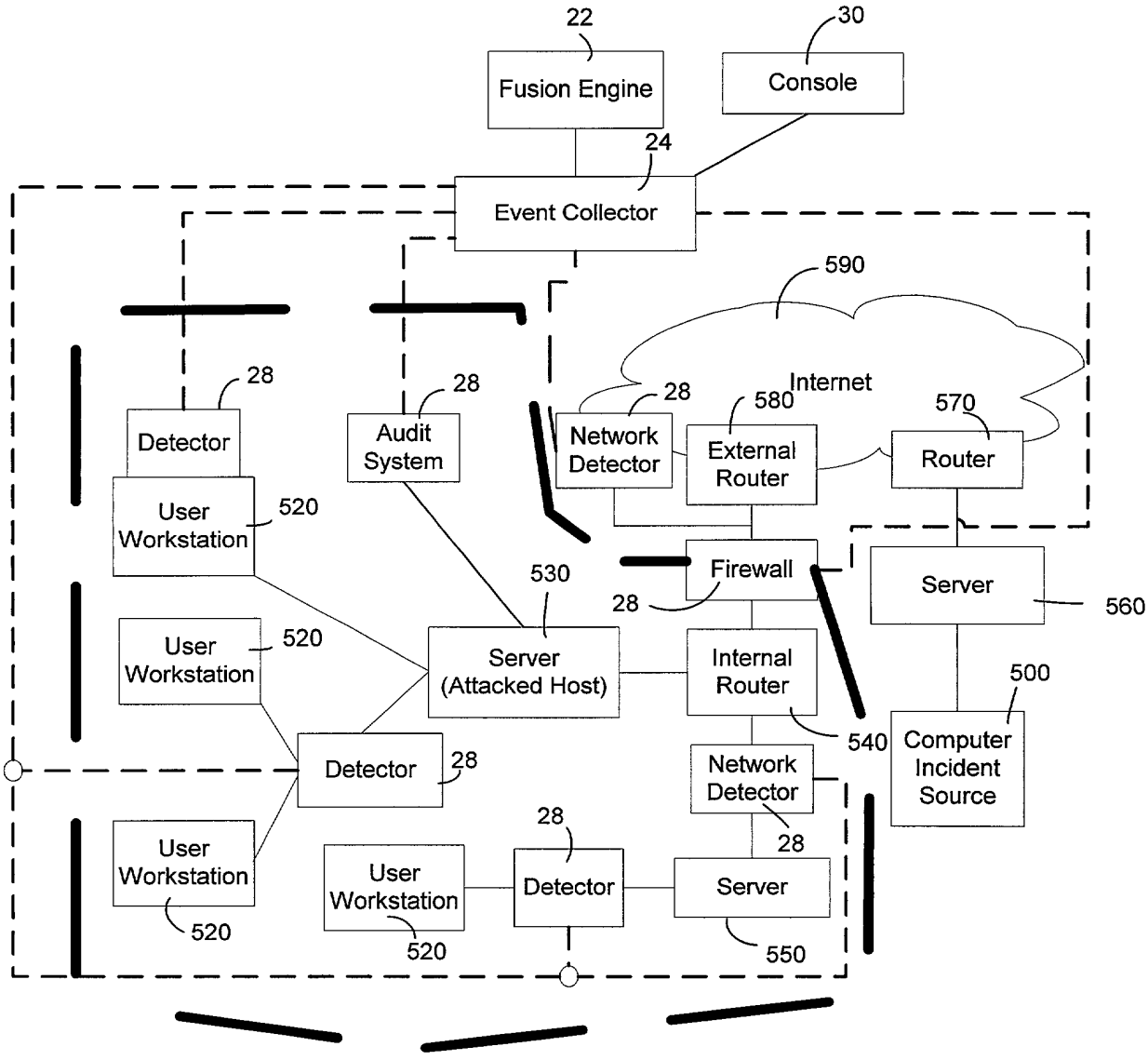
22
Fusion Engine
30
Console
24
Event Collector
590
Internet
28
Detector
28
Audit System
28
Network Detector
580
External Router
570
Router
User Workstation
520
Firewall
530
28
Server
560
User Workstation
520
Server (Attacked Host)
Internal Router
500
Detector
28
540
Computer Incident Source
Network Detector
28
User Workstation
520
28
User Workstation
520
Detector
Server
550

FIG. 5A

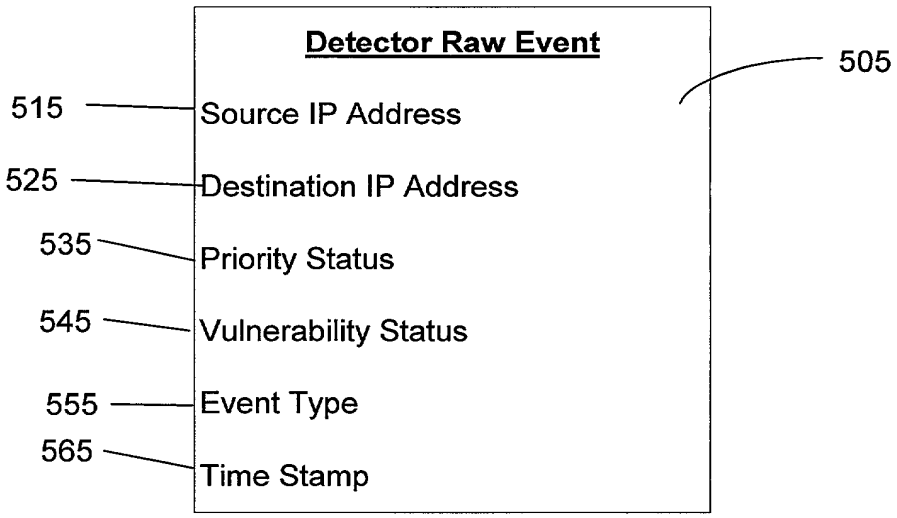
Detector Raw Event
505
515
Source IP Address
525
Destination IP Address
535
Priority Status
545
Vulnerability Status
555
Event Type
565
Time Stamp

FIG. 5B

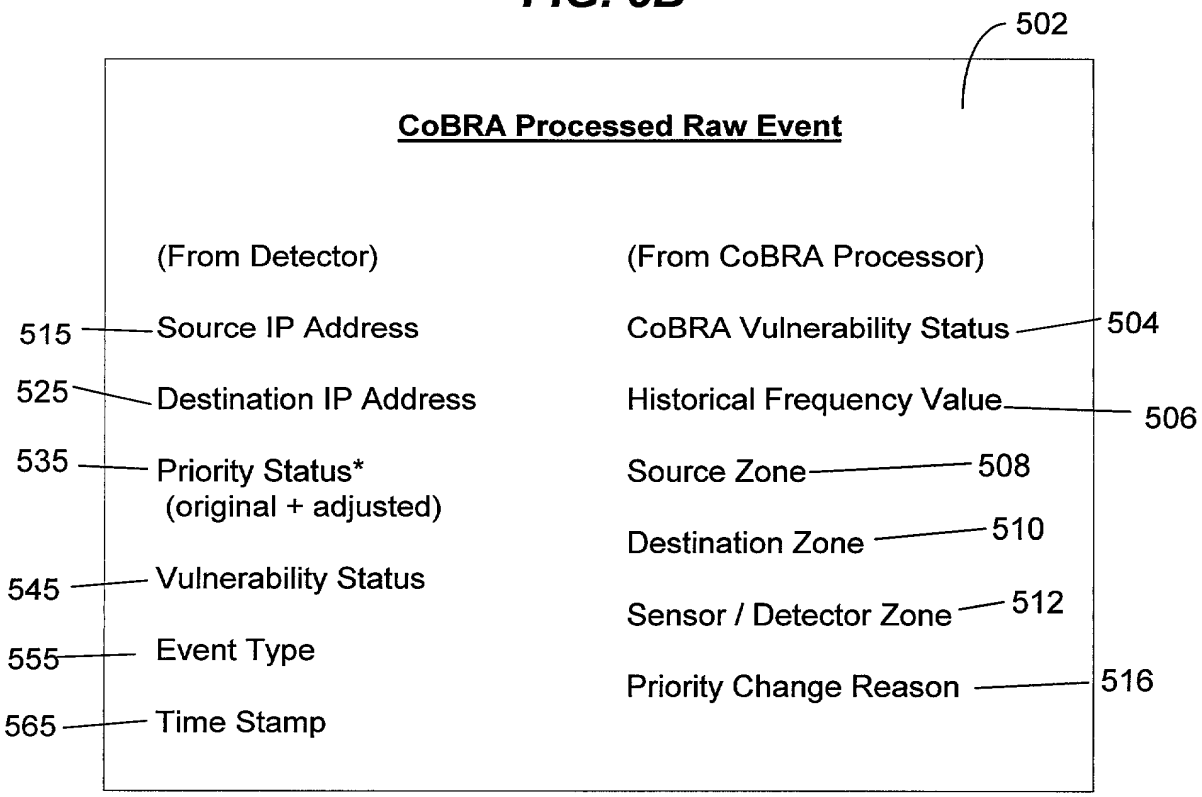
502
CoBRA Processed Raw Event
(From Detector)
(From CoBRA Processor)
515
Source IP Address
CoBRA Vulnerability Status
504
525
Destination IP Address
Historical Frequency Value
506
535
Priority Status*
(original + adjusted)
Source Zone
508
Destination Zone
510
545
Vulnerability Status
Sensor / Detector Zone
512
555
Event Type
Priority Change Reason
516
565
Time Stamp

FIG. 5C

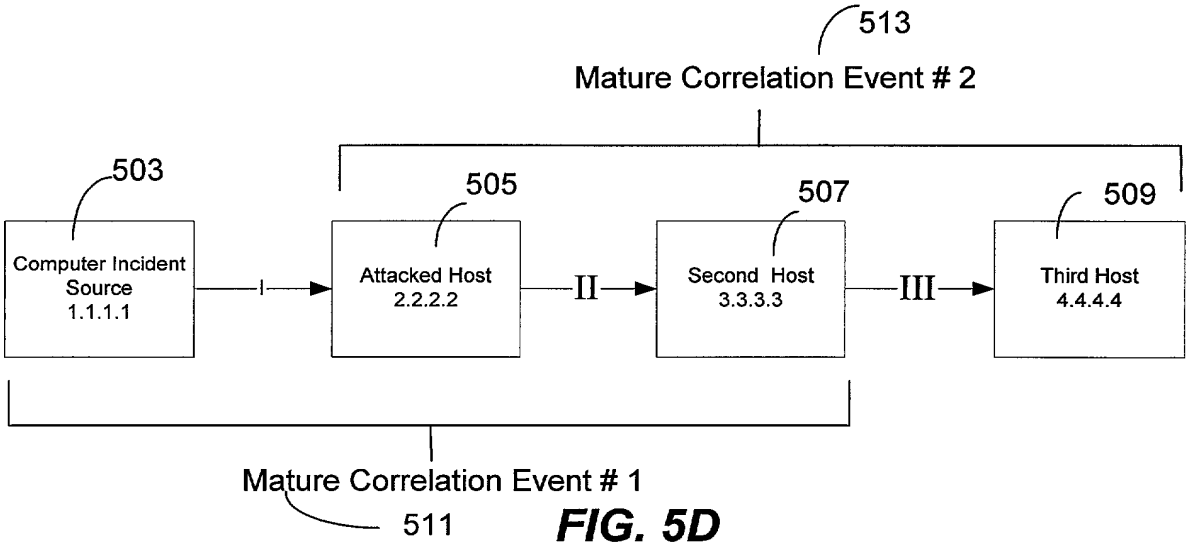

FIG. 5D

Correlation Event #1 — 511

Inbound Attacks:
Raw Event I:
Source = Computer Incident Source (1.1.1.1)
Destination = Attacked Host (2.2.2.2)

Outbound Attacks:
Raw Event II:
Source = Attacked Host (2.2.2.2)
Destination = Second Host (3.3.3.3)

FIG. 5E

Correlation Event #2 — 513

Inbound Attacks:
Raw Event II:
Source = Attacked Host (2.2.2.2)
Destination = Second Host (3.3.3.3)

Outbound Attacks:
Raw Event III:
Source = Second Host (3.3.3.3)t
Designation = Third Host (4.4.4.4)

FIG. 5F

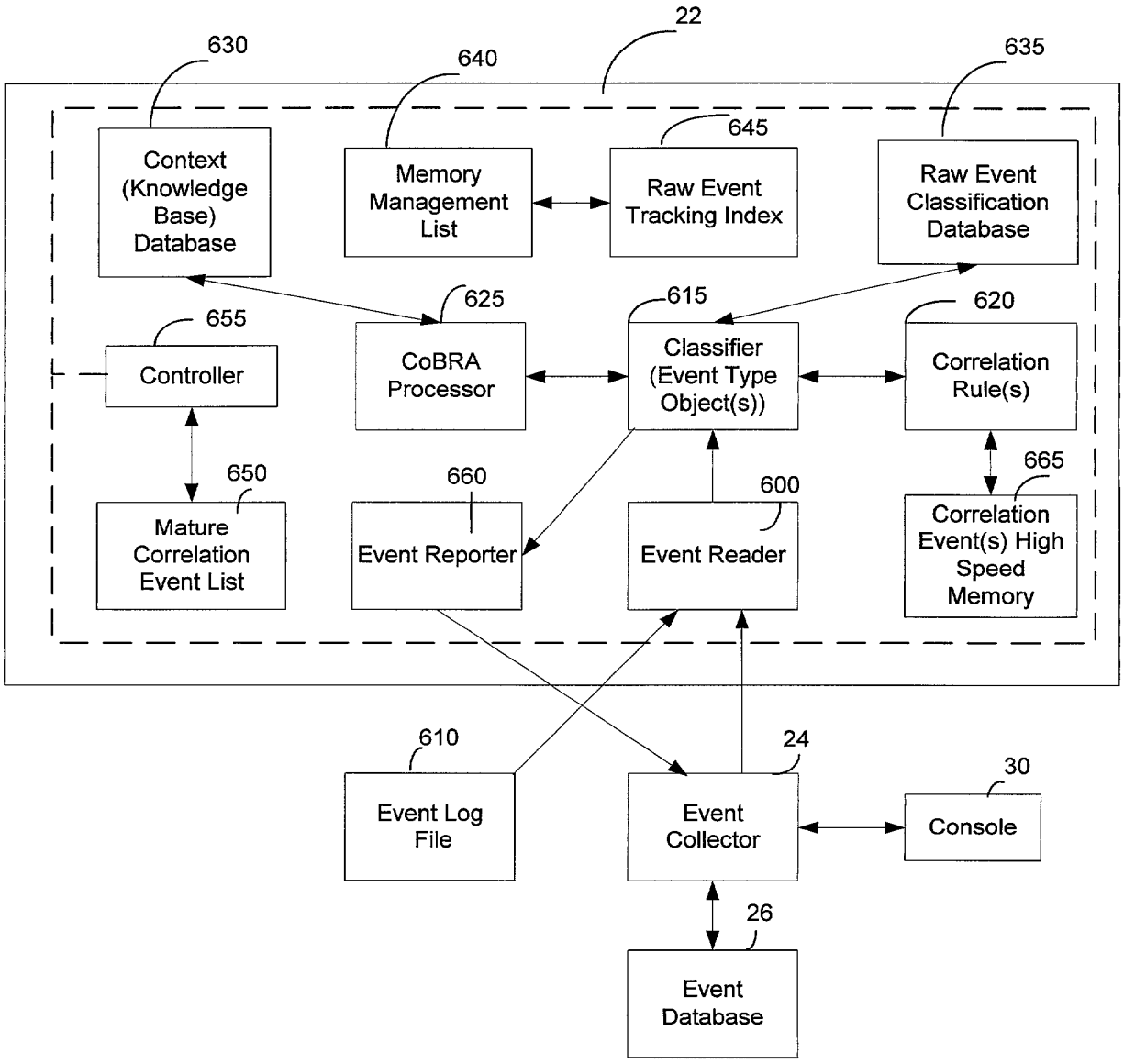
22
630
640
635
645
Context (Knowledge Base) Database
Memory Management List
Raw Event Tracking Index
Raw Event Classification Database
625
615
620
655
Controller
CoBRA Processor
Classifier (Event Type Object(s))
Correlation Rule(s)
650
660
600
665
Mature Correlation Event List
Event Reporter
Event Reader
Correlation Event(s) High Speed Memory
610
24
30
Event Log File
Event Collector
Console
26
Event Database

FIG. 6

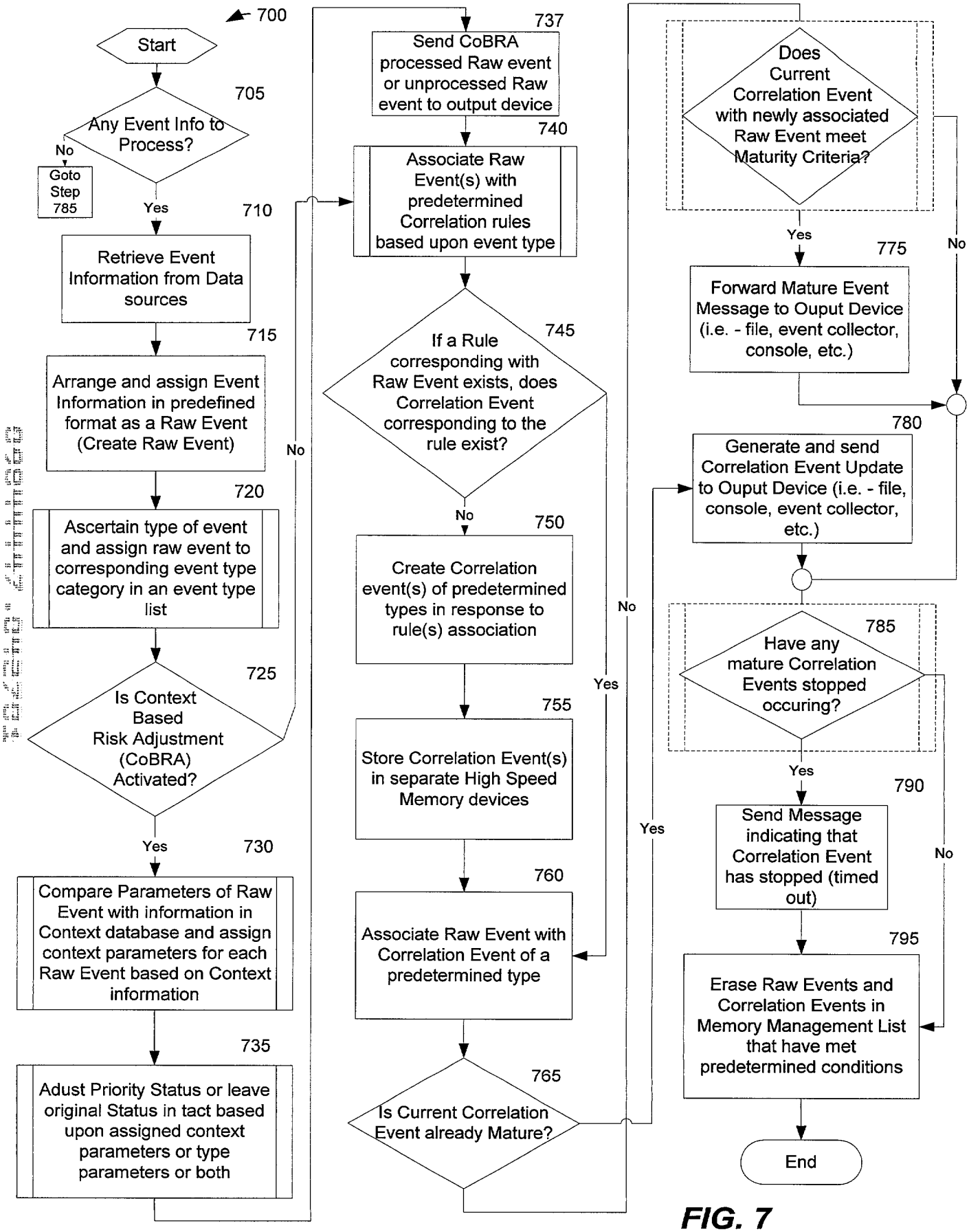
700
Start
705
Any Event Info to Process?
No
Goto Step 785
Yes
710
Retrieve Event Information from Data sources
715
Arrange and assign Event Information in predefined format as a Raw Event (Create Raw Event)
720
Ascertain type of event and assign raw event to corresponding event type category in an event type list
725
Is Context Based Risk Adjustment (CoBRA) Activated?
No
Yes
730
Compare Parameters of Raw Event with information in Context database and assign context parameters for each Raw Event based on Context information
735
Adust Priority Status or leave original Status in tact based upon assigned context parameters or type parameters or both
737
Send CoBRA processed Raw event or unprocessed Raw event to output device
740
Associate Raw Event(s) with predetermined Correlation rules based upon event type
745
If a Rule corresponding with Raw Event exists, does Correlation Event corresponding to the rule exist?
No
Yes
750
Create Correlation event(s) of predetermined types in response to rule(s) association
755
Store Correlation Event(s) in separate High Speed Memory devices
760
Associate Raw Event with Correlation Event of a predetermined type
765
Is Current Correlation Event already Mature?
No
Yes
Does Current Correlation Event with newly associated Raw Event meet Maturity Criteria?
Yes
No
775
Forward Mature Event Message to Ouput Device (i.e. - file, event collector, console, etc.)
780
Generate and send Correlation Event Update to Ouput Device (i.e. - file, console, event collector, etc.)
785
Have any mature Correlation Events stopped occuring?
Yes
No
790
Send Message indicating that Correlation Event has stopped (timed out)
795
Erase Raw Events and Correlation Events in Memory Management List that have met predetermined conditions
End

FIG. 7

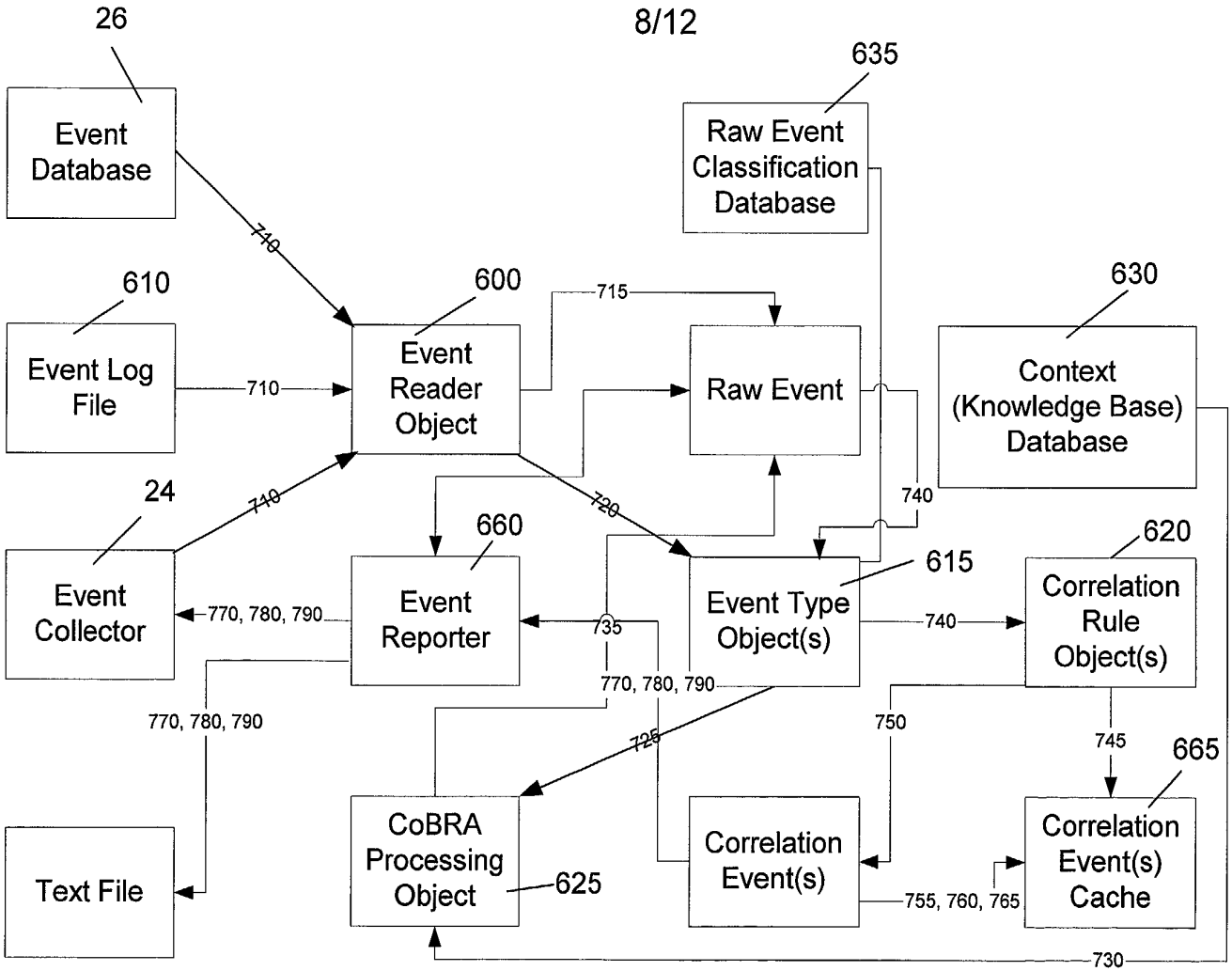
26
Event Database
635
Raw Event Classification Database
610
Event Log File
600
Event Reader Object
630
Context (Knowledge Base) Database
Raw Event
24
Event Collector
660
Event Reporter
615
Event Type Object(s)
620
Correlation Rule Object(s)
665
Correlation Event(s) Cache
CoBRA Processing Object
625
Correlation Event(s)
Text File
740
710
715
720
735
745
750
755, 760, 765
730
770, 780, 790
725

FIG. 8

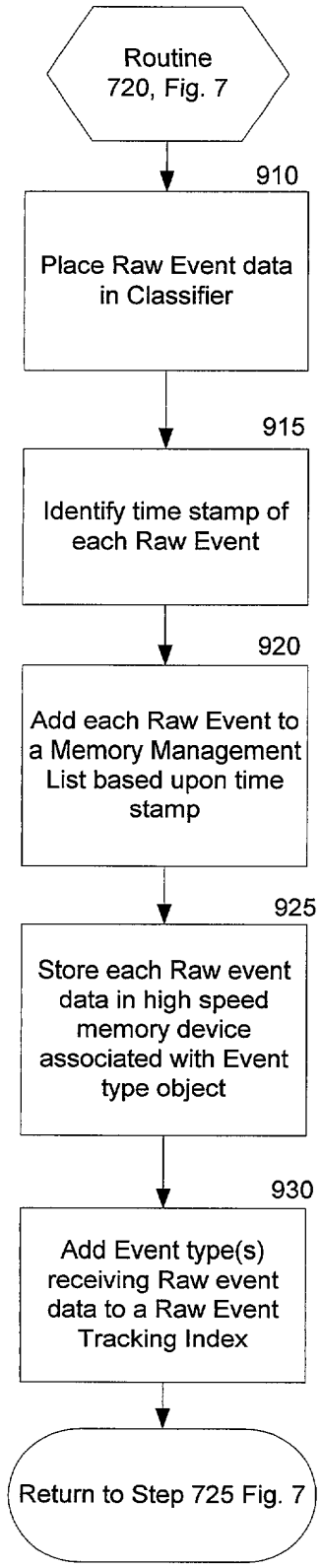
Routine 720, Fig. 7
910
Place Raw Event data in Classifier
915
Identify time stamp of each Raw Event
920
Add each Raw Event to a Memory Management List based upon time stamp
925
Store each Raw event data in high speed memory device associated with Event type object
930
Add Event type(s) receiving Raw event data to a Raw Event Tracking Index
Return to Step 725 Fig. 7

FIG. 9

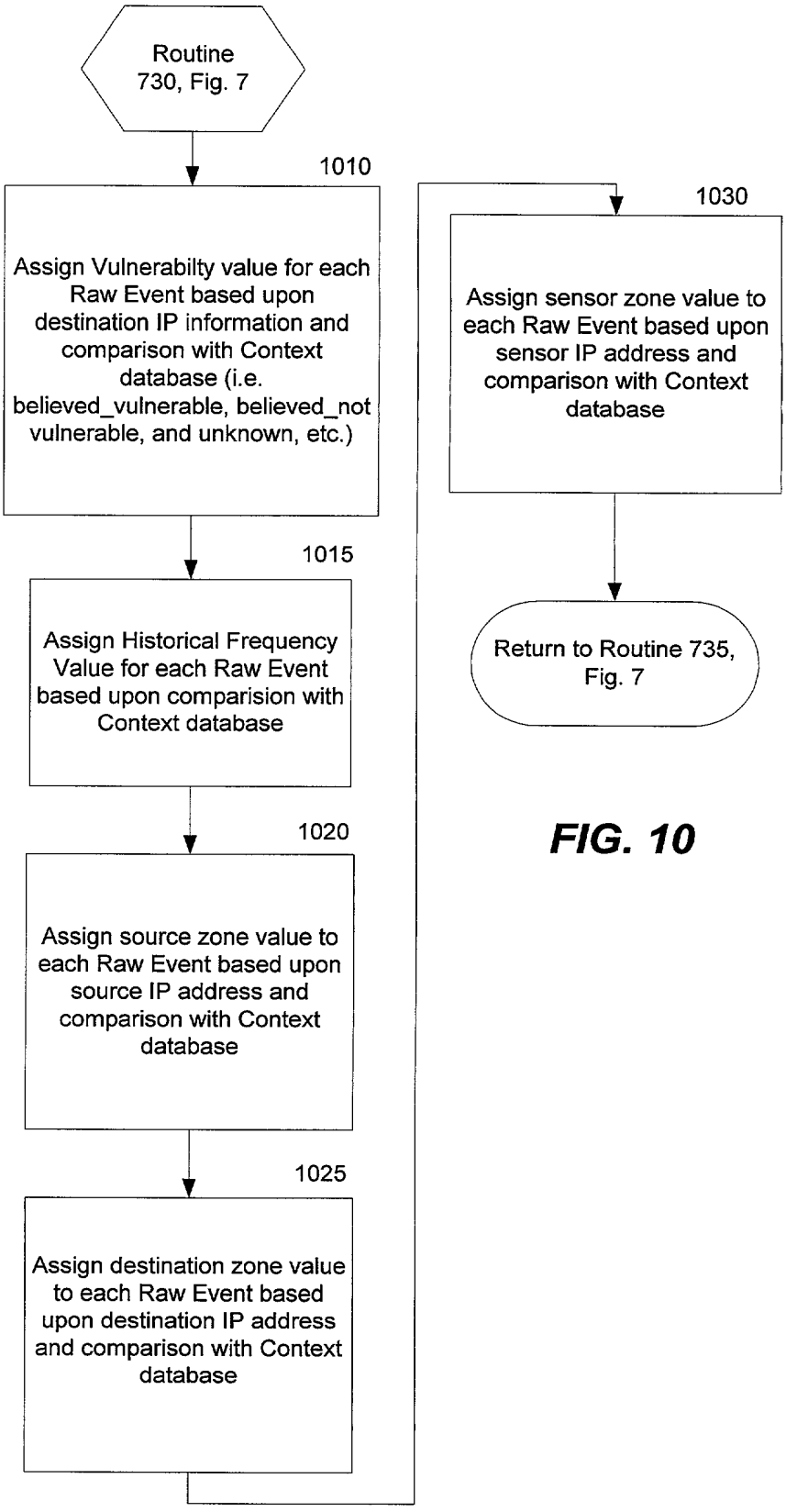
Routine 730, Fig. 7
1010
Assign Vulnerabilty value for each Raw Event based upon destination IP information and comparison with Context database (i.e. believed_vulnerable, believed_not vulnerable, and unknown, etc.)
1015
Assign Historical Frequency Value for each Raw Event based upon comparision with Context database
1020
Assign source zone value to each Raw Event based upon source IP address and comparison with Context database
1025
Assign destination zone value to each Raw Event based upon destination IP address and comparison with Context database
1030
Assign sensor zone value to each Raw Event based upon sensor IP address and comparison with Context database
Return to Routine 735, Fig. 7

FIG. 10

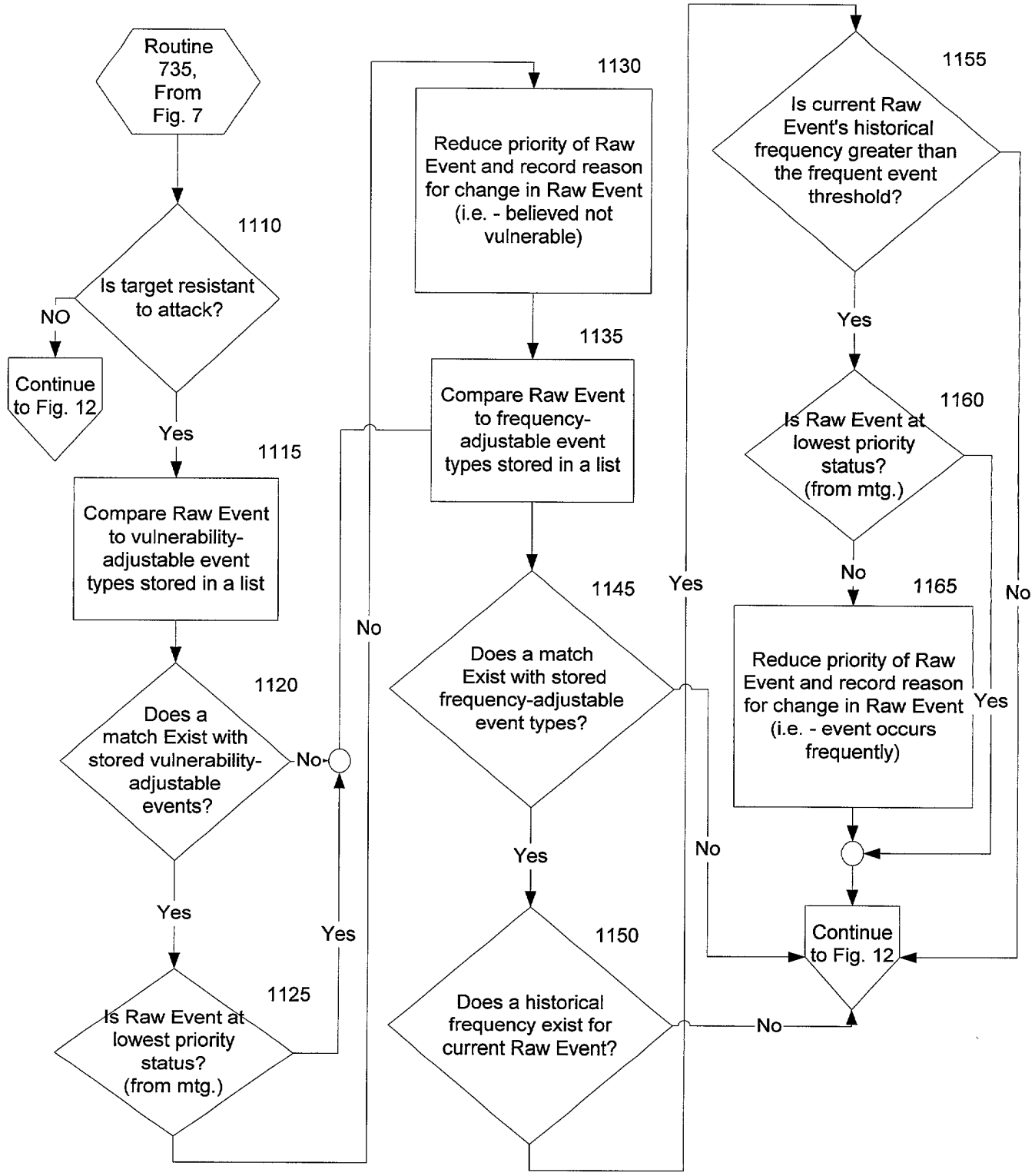
Routine 735, From Fig. 7
1110
Is target resistant to attack?
NO
Continue to Fig. 12
Yes
1115
Compare Raw Event to vulnerability-adjustable event types stored in a list
1120
Does a match Exist with stored vulnerability-adjustable events?
No
Yes
1125
Is Raw Event at lowest priority status? (from mtg.)
Yes
No
1130
Reduce priority of Raw Event and record reason for change in Raw Event (i.e. - believed not vulnerable)
1135
Compare Raw Event to frequency-adjustable event types stored in a list
1145
Does a match Exist with stored frequency-adjustable event types?
Yes
No
1150
Does a historical frequency exist for current Raw Event?
No
Yes
1155
Is current Raw Event's historical frequency greater than the frequent event threshold?
Yes
No
1160
Is Raw Event at lowest priority status? (from mtg.)
No
Yes
1165
Reduce priority of Raw Event and record reason for change in Raw Event (i.e. - event occurs frequently)
Continue to Fig. 12

FIG. 11

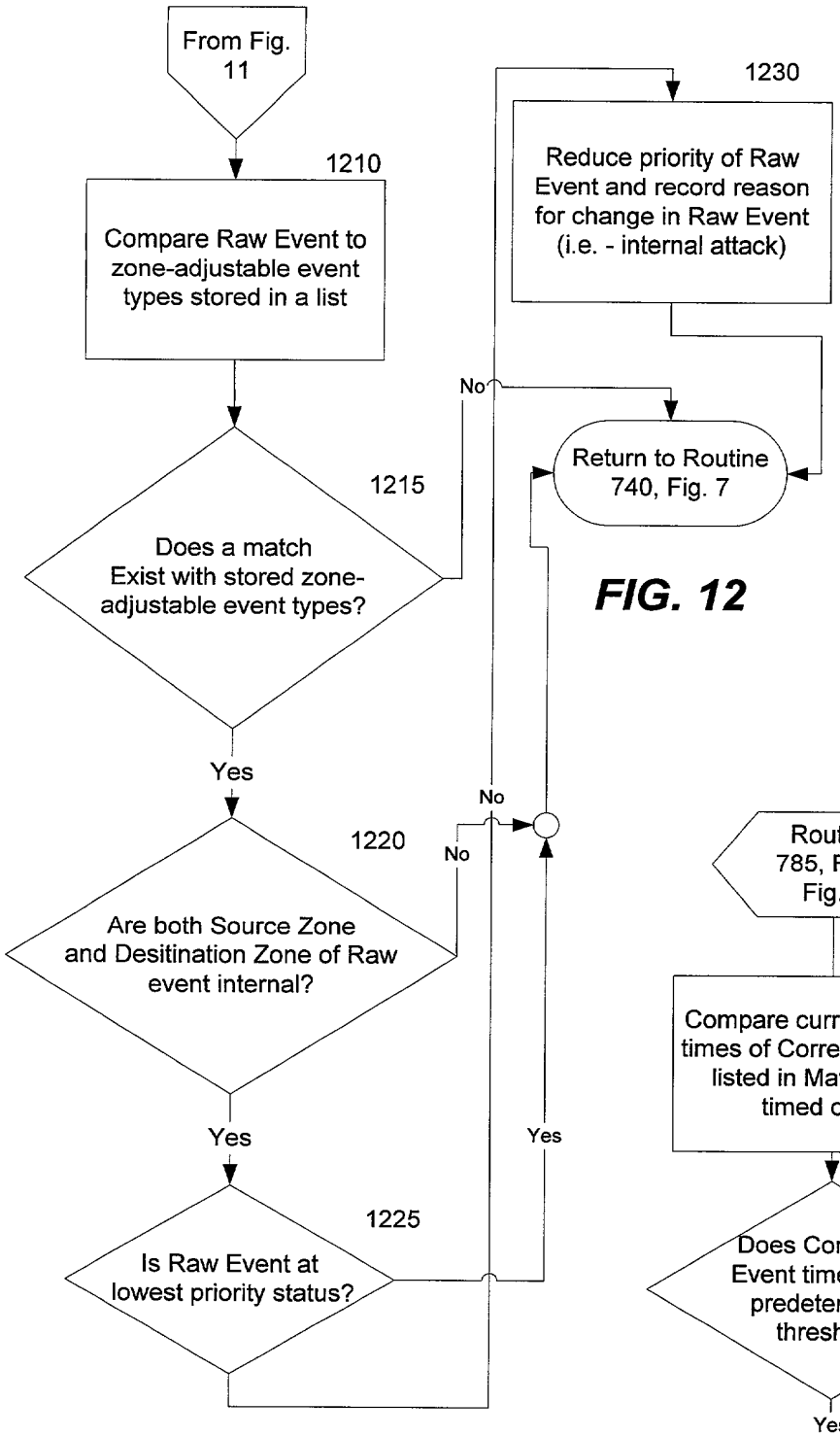

FIG. 12

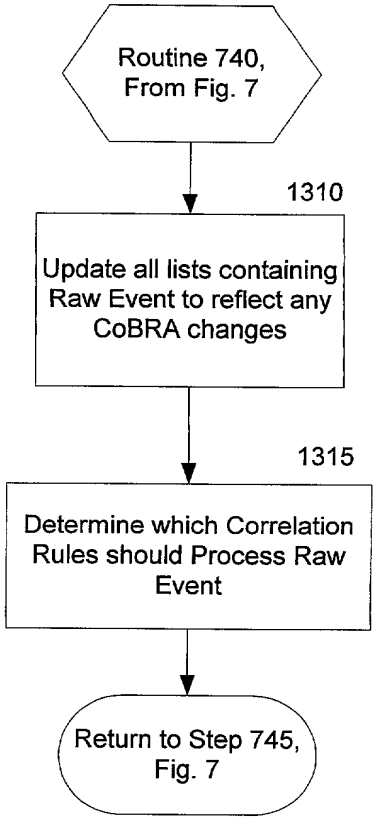

FIG. 13

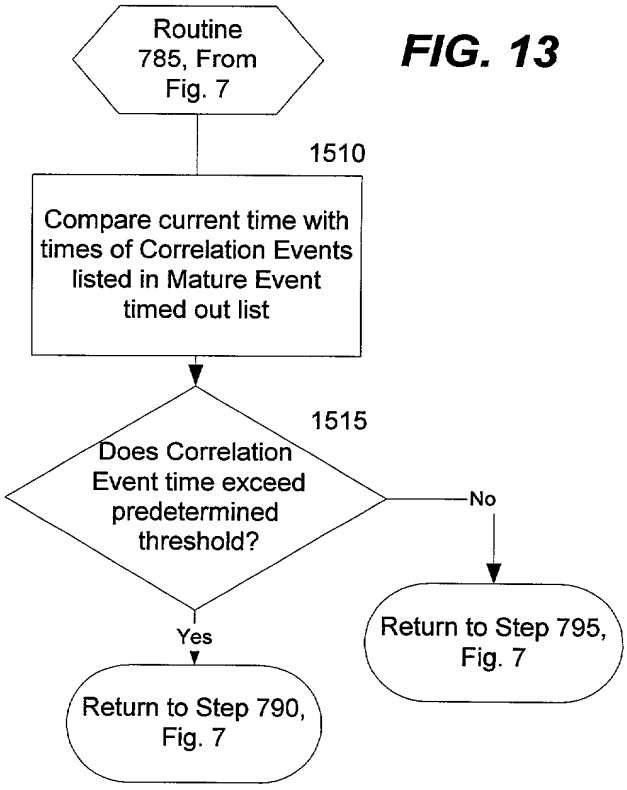

FIG. 15

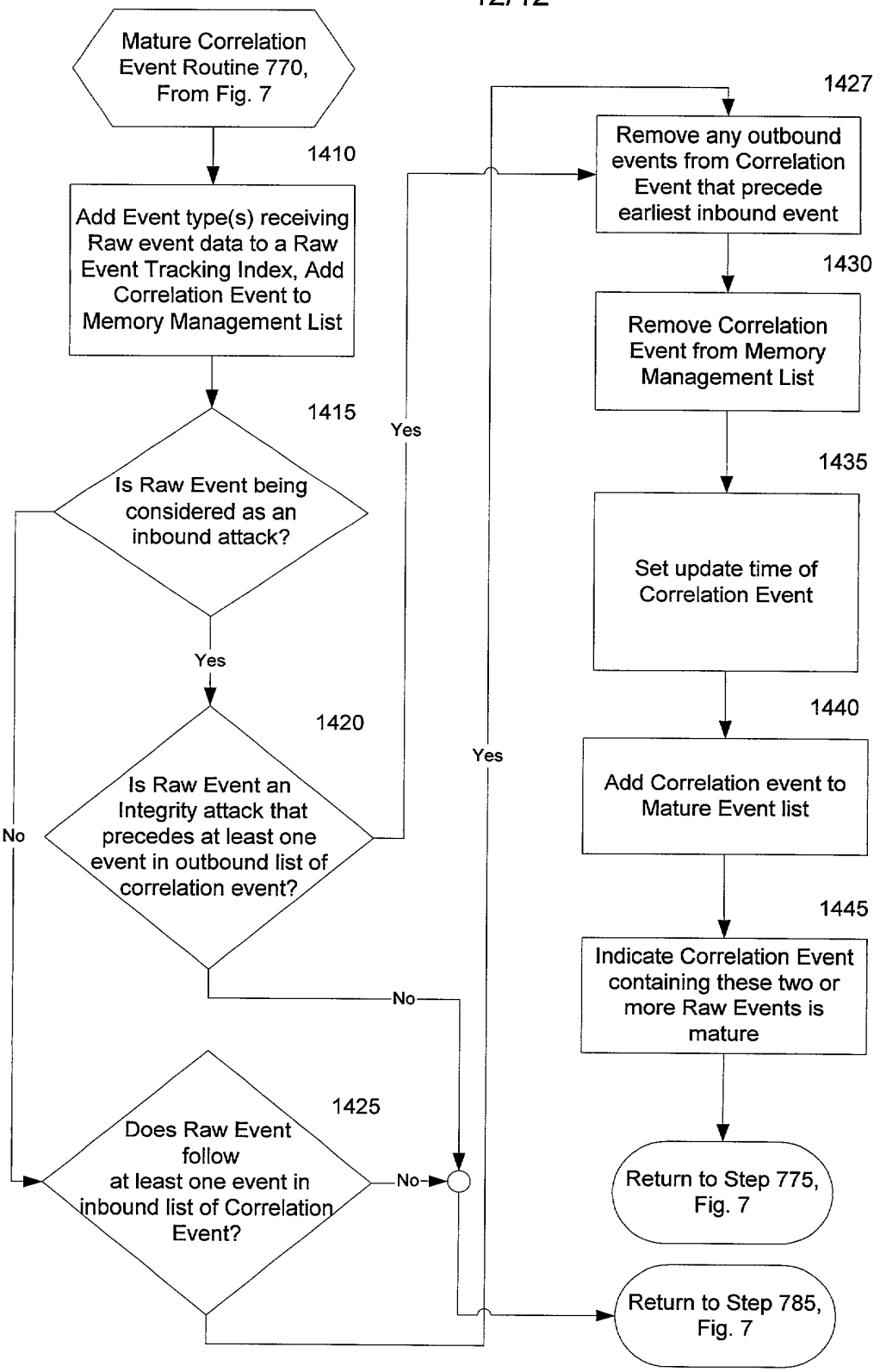
Mature Correlation Event Routine 770, From Fig. 7
1410
Add Event type(s) receiving Raw event data to a Raw Event Tracking Index, Add Correlation Event to Memory Management List
1415
Is Raw Event being considered as an inbound attack?
Yes
No
1420
Is Raw Event an Integrity attack that precedes at least one event in outbound list of correlation event?
Yes
No
1425
Does Raw Event follow at least one event in inbound list of Correlation Event?
No
1427
Remove any outbound events from Correlation Event that precede earliest inbound event
1430
Remove Correlation Event from Memory Management List
1435
Set update time of Correlation Event
1440
Add Correlation event to Mature Event list
1445
Indicate Correlation Event containing these two or more Raw Events is mature
Return to Step 775, Fig. 7
Return to Step 785, Fig. 7

FIG. 14